

Phishing alert: Don't get scammed!

If you receive an e-mail that appears to be from NAFCU and instructs you to go online to provide or “verify” financial or sensitive personal information, don't believe it: **NAFCU will never send you an e-mail asking for your credit- or debit-card, credit union or bank account information, Social Security number, login information (such as a PIN) or similarly sensitive data.**

NAFCU's name, logo, and other graphics have been used fraudulently in numerous phishing e-mails aimed at tricking people into providing sensitive financial and personal data on replicated Web sites. Giving these phishers your account and other sensitive information may expose you to identity theft and other types of fraud. If you have already complied with a phishing e-mail, you should contact the institution where you maintain your account and have the information changed immediately.

NAFCU has reported the phishing e-mail activity to the Internet Crime Complaint Center run by the FBI and the National White Collar Crime Center. Recipients are also encouraged to report these incidents; that can be done online at www.ic3.gov.

If you think you have received a phishing e-mail but are not certain, you may contact our Member Service Center at 800-344-5580; or by e-mail to msc@nafcu.org.

For information about the complaint-filing process at ICCC, go to www.ic3.gov/faq/

Related Links

[Internet Crime Complaint Center](#)
[Internet Crime Complaint Center FAQs](#)